Volume 3. Air Operator Technical Administration

CHAPTER 11. OPERATOR RECORDKEEPING

SECTION 1. GENERAL

1771. GENERAL. This chapter contains information and guidance to be used by principal operations inspectors (POI) when evaluating an operator's recordkeeping system (see volume 3, chapter 15, section 1, paragraph 2079 for definitions of accepted and approved material). This section contains a general overview of proprietary information, the regulatory requirements for recordkeeping under Title 14 of the Code of Federal Regulations (14 CFR) parts 121, 125, and 135, and definitions of terms as they relate to operator recordkeeping. Section 2 contains information and guidance about the acceptance or approval of an operator's recordkeeping system. Section 3 contains information and guidance about currency periods for records. Section 4 contains information about computer-based recordkeeping and digital and/or electronic signature use.

1773. CHARACTERISTICS OF INFORMATION AND RECORDS. Operators collect and use both information and records in the conduct of operations.

A. Information Versus Record. Inspectors should be aware of the difference between a recordkeeping system and a management information system. A record is defined as an account which preserves evidence of the occurrence of an event. In general, a record must show what event occurred, to whom, by whom, when, and proof of the event's occurrence, such as a certification by signature or by electronic means. A system that collects related information for making operational decisions but does not preserve evidence of the event's occurrence is not a recordkeeping system.

B. Proprietary Information. Proprietary information is that information which is the sole property of the operator. Inspectors do not have a right to compel an operator to divulge proprietary information. Questions about what information the operator must provide and what information the operator may withhold should be referred to Regional Counsel. Inspectors frequently acquire proprietary information in the process of conducting inspections and investigations. Inspectors may use such information for official purposes but may not divulge such information to third parties. For example, if an operator chooses to maintain flight and rest records on a payroll form, the operator must make the record available for inspection. Inspectors must take care not to divulge information such as rates of pay or dollar amounts.

1775. REGULATORY REQUIREMENTS. Parts 121, 125, and 135 require that operators maintain certain records on crewmembers and dispatchers participating in flight operations. Parts 121, 125, and 135 also specify certain regulatory requirements for recordkeeping.

A. Part 121. 14 CFR part 121, § 121.683 requires that operators maintain current records to show that each crewmember and dispatcher, as applicable, complies with proficiency and qualification requirements as stated in this chapter. Section 121.683 also requires that operators record each action taken concerning the release from employment or physical or professional disqualification of any flight crewmember or dispatcher and retain that record for 6 months. Section 121.683 does not specify time periods that qualification records must be kept other than those in § 121.683(a)(2). This section also provides for approval of computer-based record systems by the Administrator to comply with the recordkeeping requirements of that section (operations specification (OpSpec) A025). Sections 121.695 and 121.697 specify retention periods for load manifests, flight or dispatch releases, and flight plans. Section 121.711 specifies the retention period of en route radio contact between the operator and the operator's pilots.

B. Part 135. 14 CFR part 135, § 135.63 requires that operators keep certain records at either the prin-

cipal business office or another place approved by the Administrator, and establish retention periods for certain required records.

C. Part 125. 14 CFR part 125 § 125.401(c) requires that operators maintain current records to show that each crewmember complies with proficiency and qualification requirements. Part 125 subpart L, Records and Reports, specifies requirements for other forms, reports, logs, records, and signature authorities.

D. Other. In order for an operator to show regulatory compliance and to allow the Federal Aviation Administration (FAA) to conduct surveillance to determine this compliance, the operator may elect to maintain other types of records, such as extended-range operations with two-engine airplanes (ETOPS) and navigation records, even though they are not specifically mentioned in parts 121 and 135. Other examples are company flight instructor/check airman training records, school designated examiners (SDE), and aircrew program designees (APD).

1777. DEFINITIONS. The following definitions are used throughout this chapter:

A. Authentication. The means by which a system validates the identity of an authorized user. These may include a password, a personal identification number (PIN), a cryptographic key, a badge, or a stamp.

B. Calendar Month. The first day through the last day of a particular month.

C. Computer-based Recordkeeping System. A system of record processing in which records are entered, stored, and retrieved electronically by a computer system rather than in traditional hard copy form.

D. Computer Hardware. A computer and the associated physical equipment directly involved in the performance of communications or data processing functions.

E. Computer Software. Written or printed data, such as programs, routines, and symbolic languages essential to the operation of computers.

F. Control. A person has control of a transferable record if a system employed for evidencing the transfer of interests in the transferable record reliably establishes that person as the person to which the transferable record was issued or transferred.

G. Conditions. A system satisfies "control," and a person is deemed to have control of a transferable record, if the transferable record is created, stored, and assigned in such a manner that:

(1) a single authoritative copy of the transferable record exists which is unique, identifiable, and except as otherwise provided in paragraphs (4), (5), and (6), unalterable;

(2) the authoritative copy identifies the person asserting control as:

(a) the person to whom the transferable record was issued; or

(b) if the authoritative copy indicates that the transferable record has been transferred, the person to which the transferable record was most recently transferred;

(3) the authoritative copy is communicated to and maintained by the person asserting control or its designated custodian;

(4) copies or revisions that add or change an identified assignee of the authoritative copy can be made only with the consent of the person asserting control;

(5) each copy of the authoritative copy and any copy of a copy is readily identifiable as a copy that is not the authoritative copy; and

(6) any revision of the authoritative copy is readily identifiable as authorized or unauthorized.

H. Data Backup. Use of one of several recognized methods of providing a secondary means for storing records. This backup can be used to reconstruct the format and content of electronically stored records in case of loss of, failure of, or damage to the primary recordkeeping system.

I. Database Management System (DBMS). A computer software program capable of maintaining stored information in an ordered format, manipulating that data by mathematical methods, and performing data processing functions such as retrieval of data.

J. Data Entry. The process by which data or information is entered into a computer memory or storage medium. Sources include manually-written records, real-time information, and computer-generated data.

K. Data Verification. A process of assuring accuracy of data records by systematically or randomly

comparing electronic records with manual data entry documents.

L. Digital Signature. Digital signature technology is the foundation of a variety of security, e-business, and e-commerce products. Based on public/private key cryptography, digital signature technology is used in secure messaging, public key infrastructure (PKI), virtual private networks (VPN), web standards for secure transactions, and digital signatures.

M. Electronic Mail. The transmittal of messages, documents, or other communications between computer systems or other telecommunication channels.

N. Electronic Record. A contract, Operation Specification Paragraph (OpSpec), or other record created, generated, sent, communicated, received, or stored by electronic means.

O. Electronic Signature. An electronic sound, symbol, or process attached to, or logically associated with, a contract or other record and executed or adopted by a person with the intent for electronically identifying individuals entering, verifying, or auditing computer-based records, and checking for authenticity. An electronic signature combines cryptographic functions of a digital signature with the image of a person's handwritten signature or some other form of visible mark that would be considered acceptable in a traditional signing process, authenticates data, and provides permanent secure user-authentication.

P. Electronic Technology. Relating to or having electrical, digital, magnetic, wireless, optical, electromagnetic or similar capabilities.

Q. Eligibility (Grace) Period. Three calendar months: the calendar month before the training/checking month, the training/checking month, and the calendar month after the training/checking month. During this period, a crewmember or aircraft dispatcher must receive recurrent training, a flight check, or a competency check to remain in a qualified status. Training or checking completed during the eligibility period is considered to be completed during the training/checking month (base month). For example, if a crewmember or aircraft dispatcher whose training/checking month is August receives the required recurrent training in September, August remains as the training/checking month. Also, if a crewmember or aircraft dispatcher fails to complete the required training during the grace period and acquires flight time or functions as a dispatcher during the month following the training/checking month, the crewmember or aircraft dispatcher is not in violation of 14 CFR since the month following the training/checking month is still considered part of the grace period.

R. Modem. A device that can use existing telephone transmission circuits to transfer information between either two or more computer systems, or computers and remote terminals.

S. Password. An identification code required to access stored material. A device intended to prevent information from being viewed, edited, or printed by unauthorized persons.

T. Proprietary Information. Information which is the private property of the operator.

U. Real-Time Record. Information that is entered into a computer-based recordkeeping system immediately following the completion of an event or fulfillment of a condition, without first relying on the manual recording of the information on a data entry form.

V. Records. Information in a predetermined format that shows that the operator or its personnel have accomplished a particular event, have met certain criteria, or have fulfilled specific conditions required by the regulations.

W. System Security. Policies, procedures, and system structures designed to prevent users from gaining access to sections of a database to which they are not authorized access.

X. Telephone Dial-In Access. A means of gaining access to a computer system from a remote location through a telephone modem and existing telephone circuits.

Y. Training/Checking Month (Base Month). The calendar month during which a crewmember or aircraft dispatcher is due to receive required recurrent training, a required check, or a required familiarization flight.

Z. User Identification. A series of alphabetic and/or numeric characters assigned to one or more individuals or organizations for the purpose of gaining access to a computer system and accounting for time usage.

1779. MERGERS AND ACQUISITIONS. When two or more computer-based recordkeeping systems are being consolidated because of a merger or acquisition, the consolidation of the training programs and the recordkeeping systems which correlate to those

programs is of particular importance. Accurate consolidation of those systems must be given priority by the POI. Training records of the acquired company's flight operations personnel must comply with the basic 14 CFR requirements before being accepted. Once the surviving system has been approved, the operator should transfer data from the existing system into the surviving system.

A. Unavailable Records. Due to variances in recordkeeping methods of individual operators, some records may not be available or usable for inclusion in the surviving computer-based recordkeeping system. In this case, the operator must reconstruct records from available resources. If there are no resources from which to reconstruct records, assumptions that experienced personnel have accomplished required training may be required. In these cases, the POI and operator should agree on a method of identifying portions of a record that are based on these assumptions. The method used to identify this information should be discussed in the operator's user manual.

B. Changes to Existing Recordkeeping System. The POI is responsible for evaluating any request for change to an operator's existing recordkeeping system. Minor changes such as modifications to display formats may not require a formal evaluation and approval. Major changes affecting system operation or capability may require an in-depth evaluation and approval process.

C. Transition from Existing System to Surviving System. The transition procedures from the operator's existing system to the surviving system must be approved by the POI. During this transition, the POI shall determine the time period required for maintaining the two systems in parallel operation. The surviving system should have at least the same backup capability as the existing system. The integration of the existing and surviving systems may be accomplished by electronically combining the databases of the two systems or by other methods, as long as the accuracy of the data is maintained.

NOTE: A change in computer hardware which does not affect functions or capabilities of the system does not constitute a system transition and does not require approval.

1780. - 1790. RESERVED.

[PAGES 3-955 THROUGH 3-956 RESERVED]